REMARKS

This amendment is submitted in response to the Office Action of June 7, 2004. Reconsideration and allowance of the claims is requested.

In the Office Action claims 1-4, 9 were withdrawn; the remainder were considered and rejected. These rejections are considered below.

Claims 5 and 13 were objected to; these objections are overcome by adopting the Examiner's suggestions.

Claims 5-8 and 10-17 are rejected under 35 U.S.C. 112 as indefinite. The issues raised as to the clarity of the claim language in claims 5, 12 and 13 have been dealt with.

Claims 5 and 6 are rejected as non-statutory. This rejection is traversed. The claims are amended to clarify the use of a PEAD in implementing the method, thereby eliminating the Examiner's argument.

The existence of allowable subject matter in claims 13-17 is acknowledged.

Claims 5-8 and 10-11 are rejected under 35 U.S.C. 102 as anticipated by *Dorenbos*, U.S. Patent 5,751,813; claim 12 is rejected as obvious over *Dorenbos* taken with *Spies et al.*, U.S. Patent 6,055,314. These rejections are respectfully traversed.

Apparently Examiner does not appreciate what is "shared secret." In Dorenbos' col. 3, lines 12-15, does not teach anything about generating a shared secret. A shared secret in cryptography usually refers to a encryption/decryption key generated by a sender's private key and a receiver's public key or generated by a sender's public key and a receiver's private key. Mathematically we can show that a shared secret generated by a sender's private key and receiver's public key is equal to a shared secret generated by a sender's public key and receiver's private key. The security is built without exchanging sender's and receiver's private keys; both parties can derived a common shared secret just using each other's public key which available in public. In Dorenbos' col. 3, lines 12-15, simply appending sender's ID or receiver's ID cannot generate a shared secret. Furthermore, a shared secret is totally independent of both parties IDs.

No encryption server is involved when sender encrypting a message with a shared secret in our invention. In Dorenbos' col. 3, lines 34-36, the encryption server

uses recipient public key to encrypt the message not a share secret derived from both parties.

As described above, a receiver can use its own private key and sender's public key to derive a shared secret. In Dorenbos' col. 4, lines 4-10, for each recipient, the encryption server just use the recipient's public key to encrypt the message.

Having addressed all issues set out in the office action, Applicant respectfully submits that the claims are in condition for allowance and respectfully request that the claims be allowed.

Respectfully submitted,

James A. Sheridan
Registration No. 25,435
MOSER, PATTERSON & SHERIDAN, L.L.P.
595 Shrewsbury Ave. Suite 100
Shrewsbury, NJ 07702
Telephone: (650) 330-2310
Facsimile: (650) 330-2314